ABSTRACT OF THE DISCLOSURE

A system and method distribute the task of decryption between a server and a client. To encrypt data, the client generates an encryption/decryption key. Namely, a user interface obtains a password, generally from a user. A hint generator generates a hint. A key generator generates the key based on the password and the hint. In one embodiment, the key generator hashes the password to generate a first secret, hashes the first secret to generate a second secret, hashes the first secret with the hint to generate an intermediate index, and hashes the second secret and the intermediate index to generate the key. An encryption engine can then use the key to encrypt data. The client then sends the encrypted data and possibly the hint for storage on the server. To decrypt the data, the key must be determined. Accordingly, the server knows some information and the user knows some information for decrypting the data. To generate the key, the decrypting client must first obtain rights to retrieve the hint from the server and must obtain the password from the user. Increased level of security is achieved.